Interview Summary

1. A proposed amendment was submitted for applicant's consideration. Examiner suggested Applicant to amend claims as shown in the Examiner's Amendment below in order to place the application in condition for allowance.

Examiner's Amendment

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

3. Authorization for this examiner's amendment was given in a telephone interview with the Applicant's Representative, Leon R. Turkevich (Reg. No. 34,035), on 29 February 2008.

IN THE SPECIFICATION

Please replace the paragraph on page 11, starting at line 5, as below:

Figure 4 is a diagram illustrating the method of ordering packets for a given secure connection according to quality of service requirements prior to encryption, according to an embodiment of the present invention. The steps described herein with respect to Figure 4 can be implemented as executable code stored on a computer readable storage medium (e.g., floppy disk, hard disk, EEPROM, CD-

ROM, etc.), or propagated via a computer readable transmission medium (e.g., fiber optic cable, electrically-conductive transmission line medium, wireless electromagnetic medium, etc.).

IN THE CLAIMS

Please replace all claims as shown below:

AMENDMENTS TO THE CLAIMS

1. (CURRENTLY AMENDED) A method in a router having at least one outbound interface, the method comprising:

establishing, on the outbound interface, a plurality of Internet Protocol (IP)-based secure connections with respective destinations based on receiving encrypted packets generated by a cryptographic module, each encrypted packet successively output from the cryptographic module having a corresponding successively-unique sequence number;

controlling supply of unencrypted data packets to the cryptographic module by:

(1) assigning, for each secure connection, a corresponding queuing module,

(2) reordering, in each queuing module, a corresponding group of the unencrypted data packets associated with the corresponding secure connection according to a determined quality of service policy and based on a corresponding assigned maximum output bandwidth for the corresponding queuing module, and

(3) outputting to the cryptographic module the group of unencrypted data

packets, from each corresponding queuing module according to the corresponding assigned maximum output bandwidth, for generation of the encrypted packets; and

second outputting the encrypted packets from the cryptographic module to the outbound interface for transport via their associated secure connections;

wherein the reordering step includes, in each queuing module, reordering the corresponding group of the unencrypted data packets according to the determined quality of service policy in response to detection of a congestion condition in the outbound interface.

2. (CANCELED).

3. (CURRENTLY AMENDED) The method of claim 1, wherein the reordering step includes, in each queuing module:

establishing a plurality of queues having respective identified priorities;

storing each unencrypted data packet associated with the corresponding secure connection in one of the queues based on a corresponding identified priority for said each unencrypted data packet; and

selectively outputting the stored unencrypted data packets from the queues, according to the corresponding quality of service policy.

4. (CURRENTLY AMENDED) The method of claim 1, wherein:

the establishing step includes establishing, on each of a plurality of the outbound interfaces, a corresponding plurality of the secure connections with a corresponding

plurality of respective destinations based on receiving a corresponding stream of encrypted packets from the cryptographic module;

the controlling step includes controlling the supply of unencrypted data packets, for each outbound interface, ~~from~~ to the cryptographic module based on repeating the assigning, reordering, and outputting steps for each of the secure connections;

the second outputting step including outputting each encrypted packet to a corresponding one of the outbound interfaces according to a routing decision executed by the router.

5. (ORIGINAL) The method of claim 1, wherein the second outputting step includes outputting the encrypted packets for transport via their associated secure connections according to IP Security (IPSEC) protocol.

6. (PREVIOUSLY PRESENTED) The method of claim 5, wherein the determined quality of service policy implements a guaranteed quality of service for one of a video stream or an audio stream.

7. (ORIGINAL) The method of claim 6, wherein the audio stream is a Voice over IP media stream.

8. (ORIGINAL) The method of claim 1, wherein the controlling step further includes obtaining, for each queuing module, the corresponding assigned maximum output bandwidth from a configuration register.

9. (ORIGINAL) The method of claim 1, wherein the controlling step further includes negotiating, for at least one queuing module, the corresponding assigned maximum output bandwidth with the corresponding destination.

10. (CURRENTLY AMENDED) A router comprising:

a cryptographic module configured for successively outputting encrypted packets having respective successively-unique sequence numbers;

an outbound interface configured for establishing a plurality of Internet Protocol (IP)-based secure connections with respective destinations based on receiving respective streams of the encrypted packets; and

a queue controller configured for controlling supply of unencrypted data packets to the cryptographic module, the queue controller configured for assigning, for each secure connection, a corresponding queuing module, each queuing module configured for:

(1) outputting to the cryptographic module a corresponding group of the unencrypted data packets associated with the corresponding secure connection, and according to a corresponding assigned maximum output bandwidth for the corresponding queuing module, for generation of the corresponding stream of the encrypted packets, and

(2) reordering the corresponding group of the unencrypted data packets according to a determined quality of service policy and the corresponding assigned maximum output bandwidth;

wherein each queuing module is configured for reordering the corresponding group of the unencrypted data packets in response to detection of a congestion condition in the outbound interface having established the corresponding secure connection.

11. (CANCELED).

12. (CURRENTLY AMENDED) The router of claim 10, wherein each queuing module is configured for:

establishing a plurality of queues having respective identified priorities;

storing each unencrypted data packet associated with the corresponding secure connection in one of the queues based on a corresponding identified priority for said each unencrypted data packet; and

selectively outputting the stored unencrypted data packets from the queues, according to the corresponding quality of service policy.

13. (ORIGINAL) The router of claim 10, wherein the cryptographic module is configured for outputting the encrypted packets for transport via their associated secure connections according to IP Security (IPSEC) protocol.

14. (PREVIOUSLY PRESENTED) The router of claim 13, wherein the determined quality of service policy implements a guaranteed quality of service for one of a video stream or an audio stream.

15. (ORIGINAL) The router of claim 14, wherein the audio stream is a Voice over IP media stream.

16. (ORIGINAL) The router of claim 10, wherein the queue controller includes a configuration register configured for storing, for each queuing module, the corresponding assigned maximum output bandwidth.

17. (ORIGINAL) The router of claim 10, wherein the queue controller includes a peer bandwidth module configured for negotiating, for each queuing module, the corresponding assigned maximum output bandwidth with the corresponding destination.

18. (CURRENTLY AMENDED) A computer readable storage medium having stored thereon sequences of instructions for outputting encrypted packets by a router having at least one outbound interface, the sequences of instructions including instructions for:

establishing, on the outbound interface, a plurality of Internet Protocol (IP)-based secure connections with respective destinations based on receiving encrypted packets generated by a cryptographic module, each encrypted packet successively output from the cryptographic module having a corresponding successively-unique sequence number;

controlling supply of unencrypted data packets to the cryptographic module by:

(1) assigning, for each secure connection, a corresponding queuing module,

(2) reordering, in each queuing module, a corresponding group of the unencrypted data packets associated with the corresponding secure connection according to a determined quality of service policy and based on a corresponding assigned maximum output bandwidth for the corresponding queuing module, and

(3) outputting to the cryptographic module the group of unencrypted data packets, from each corresponding queuing module according to the corresponding assigned maximum output bandwidth, for generation of the encrypted packets; and

second outputting the encrypted packets from the cryptographic module to the outbound interface for transport via their associated secure connections;

wherein the reordering step includes, in each queuing module, reordering the corresponding group of the unencrypted data packets according to the determined quality of service policy in response to detection of a congestion condition in the outbound interface.

19. (CANCELED).

20. (CURRENTLY AMENDED) The medium of claim 18, wherein the reordering step includes, in each queuing module:

establishing a plurality of queues having respective identified priorities;

storing each unencrypted data packet associated with the corresponding secure connection in one of the queues based on a corresponding identified priority for said each unencrypted data packet; and

selectively outputting the stored unencrypted data packets from the queues, according to the corresponding quality of service policy.

21. (CURRENTLY AMENDED) The medium of claim 18, wherein:

the establishing step includes establishing, on each of a plurality of the outbound interfaces, a corresponding plurality of the secure connections with a corresponding plurality of respective destinations based on receiving a corresponding stream of encrypted packets from the cryptographic module;

the controlling step includes controlling the supply of unencrypted data packets, for each outbound interface, ~~from~~ to the cryptographic module based on repeating the assigning, reordering, and outputting steps for each of the secure connections;

the second outputting step including outputting each encrypted packet to a corresponding one of the outbound interfaces according to a routing decision executed by the router.

22. (ORIGINAL) The medium of claim 18, wherein the second outputting step includes outputting the encrypted packets for transport via their associated secure connections according to IP Security (IPSEC) protocol.

23-26. (CANCELED).

27. (CURRENTLY AMENDED) A router having at least one outbound interface, the router further comprising:

means for establishing, on the outbound interface, a plurality of Internet Protocol (IP)-based secure connections with respective destinations based on receiving encrypted packets;

means for generating the encrypted packets, each encrypted packet successively output having a corresponding successively-unique sequence number; and

means for controlling supply of unencrypted data packets to the generating means, including:

(1) means for assigning, for each secure connection, a corresponding queuing means for queuing unencrypted data packets,

(2) means for reordering, in each queuing means, a corresponding group of the unencrypted data packets associated with the corresponding secure connection according to a determined quality of service policy and based on a corresponding assigned maximum output bandwidth for the corresponding queuing means, the means for reordering configured for outputting to the generating means the group of unencrypted data packets, from each corresponding queuing means according to the corresponding assigned maximum output bandwidth, for generation of the encrypted packets;

wherein the means for reordering is configured for reordering, in each queuing means, the corresponding group of the unencrypted data packets according to the determined quality of service policy in response to detection of a congestion condition in the outbound interface.

28. (CANCELED).

29. (CURRENTLY AMENDED) The router of claim 27, wherein the means for reordering is configured for, in each queuing means:

establishing a plurality of queues having respective identified priorities;

storing each unencrypted data packet associated with the corresponding secure connection in one of the queues based on a corresponding identified priority for said each unencrypted data packet; and

selectively outputting the stored unencrypted data packets from the queues, according to the corresponding quality of service policy.

30. (CURRENTLY AMENDED) The router of claim 27, wherein:

the means for establishing is configured for establishing, on each of a plurality of the outbound interfaces, a corresponding plurality of the secure connections with a corresponding plurality of respective destinations based on receiving a corresponding stream of encrypted packets from the generating means;

the controlling means is configured for controlling the supply of unencrypted data packets, for each outbound interface, based on the assigning means assigning, for each secure connection for each outbound interface, a corresponding one of the queuing means;

the router further comprises routing means for selecting one of the outbound interfaces for each said unencrypted data packet, the generating means configured for outputting each encrypted packet to the corresponding selected one of the

outbound interfaces selected by the routing means.

31. (ORIGINAL) The router of claim 27, wherein the generating means is configured for outputting the encrypted packets for transport via their associated secure connections according to IP Security (IPSEC) protocol.

32. (CANCELED).

33. (CANCELED).

34. (ORIGINAL) The router of claim 27, wherein the reordering means is configured for obtaining the corresponding assigned maximum output bandwidth from a configuration register.

35. (ORIGINAL) The router of claim 27, wherein the reordering means further includes means for negotiating, for at least one queuing means, the corresponding assigned maximum output bandwidth with the corresponding destination.

36. (PREVIOUSLY PRESENTED) The method of claim 1, wherein each secure connection is a corresponding encrypted tunnel.

37. (PREVIOUSLY PRESENTED) The router of claim 10, wherein each secure connection is a corresponding encrypted tunnel.

38. (CANCELED).

39. (PREVIOUSLY PRESENTED) The router of claim 27, wherein each secure connection is a corresponding encrypted tunnel.

40. (CURRENTLY AMENDED) The method of claim 1, wherein: the router includes the outbound interface, the cryptographic module, and each of the queuing modules;

the establishing of the IP-based secure connections, the controlling supply of unencrypted data packets, and the second outputting of the encrypted packets to the outbound interface each executed in the router.

41. (CURRENTLY AMENDED) The method of claim 1, further comprising:

selecting one of the outbound interfaces for each of the unencrypted data packets by a routing circuit in the router based on receiving the unencrypted data packets from at least one inbound interface in the router;

the second outputting including outputting each encrypted packet to the corresponding selected one of the outbound interfaces selected by the routing circuit.

42. (CURRENTLY AMENDED) The router of claim 10, further comprising a routing circuit configured for selecting one of a plurality of the outbound interfaces for

each said unencrypted data packet, the cryptographic module configured for outputting each encrypted packet to the corresponding selected one of the outbound interfaces selected by the routing circuit.

Allowable Subject Matter

4. Claims 1, 3-10, 12-18, 20-22, 27, 29-31, 34-37, and 39-42 are allowed. The following is an examiner's statement of reasons for allowance: In interpreting the claims, in light of the specification and the authorized Examiner's Amendment on 29 February 2008, the Examiner finds the claimed invention to be patentably distinct from the prior art of record.

5. In regards to statutory subject matter, the Examiner interprets the claim language of "a router" to be hardware as recited in the specification in ¶ 29 and as shown in figures 1a and 2b.

6. **Maeshima et al. (6,092,113)** teaches an IP tunnel is constructed between routers connected with the INTERNET. A bandwidth of the IP tunnel is assured by setting up a reservation resource protocol (RSVP) on the IP tunnel. Further as a traffic control of the routers and on the IP tunnel, a frequency for sending packets, which are processed by an input processor and an output processor inside of the router, is allotted based on a ratio of the reserved bandwidth in each IP tunnel, then an algorithm for controlling the traffic is simplified. Furthermore each of the routers on the IP tunnel has a function for scheduling a reservation and manages a time period at which the virtual

private network (VPN) of a type of the reservation resource protocol (RSVP) will be used, then it is possible to reserve the assurance of the bandwidth on the designated date and time in the future **(Maeshima et al., abstract, figure 2, and corresponding text).**

7. **MeLampy et al. (2003/0051130)** teaches a system for providing encryption for the rerouting of multi-media data flow packets is disclosed. Generally, a first endpoint is connected to a second endpoint, wherein the first endpoint comprises a transceiver, encryption software stored within the first endpoint defining functions to be performed by the first endpoint, and a processor. The processor is configured by the encryption software to perform the steps of: assigning a sequence number to a first multi-media data flow packet received by a first endpoint, wherein the first multi-media data flow packet is within a series of multi-media data flow packets; pseudo-randomly shuffling the sequence number of the first multi-media data flow packet; and, transmitting the pseudo-randomly shuffled sequence number to a second endpoint. These steps may be performed by a programmed controller, or other hardware, instead of, or in addition to, being performed in accordance with software **(MeLampy et al., abstract, figure 1, and corresponding text).**

8. However, the prior art of record fail to teach or suggest individually or in combination the claimed limitation, wherein the reordering step includes, in each queuing module, reordering the corresponding group of the unencrypted data packets according to the determined quality of service policy in response to detection of a congestion condition in the outbound interface, which correlates to ¶ 34 of the

applicant's specification, "If congestion is detected in an outbound interface 22, the corresponding quality of service module 26 is configured to prioritize packets to provide a guaranteed quality of service for latency-sensitive traffic. As described above, however, the prioritizing of packets by the QoS module 26 may cause reordering of the encrypted packets output by the cryptographic module 20." See also ¶ 14, 19, 33, 41, 43, 48, 49, and 51 for further explanation.

9. These limitations, in conjunction with the other limitations in the independent claims 1, 10, 18, and 27, are not specifically disclosed or remotely suggested in the prior art of record. Therefore, claims 1, 3-10, 12-18, 20-22, 27, 29-31, 34-37, and 39-42 are allowed.

10. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ranodhi Serrao whose telephone number is (571) 272-7967. The examiner can normally be reached on 8:00-4:30pm, M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rupal Dharia can be reached on (571) 272-3880. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/R. N. S./

Examiner, Art Unit 2141

3/3/2008

/William C. Vaughn, Jr./

Supervisory Patent Examiner, Art Unit 2144